UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/904,651	07/16/2001	Jian Kang Wu	24698	6197

7590   03/24/2005

NATH & ASSOCIATES PLLC
Sixth Floor
1030 Fifteenth Street, N.W.
Washington, DC 20005

EXAMINER
TRAN, TONGOC

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 03/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 July 2001*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-62* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-50 and 58-62* is/are rejected.

7)☒ Claim(s) *51-57* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage

        application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date *9/5/2001, 12/7/200.*

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____ .

DETAILED ACTION

1.   This office action is in response to Applicant's application serial no. 09/904651

filed on 7/16/2001. Claims 1-62 are pending.

Claim Objections

2.   Claim 55 is objected to because of the following informalities:

Claim 55 appears to be dependent on claim 54, not claim 34. Appropriate

correction is required.

Claim Rejections - 35 USC § 103

3.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-16 and 18-50 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Choudhury et al. (U.S. Patent No. 5,509,074) in view of Houser et al.

(U.S. Patent No. 5,606,609).

In respect to claim 1, Choudhury discloses a method for the remote printing of a

document by use of a network, the method including the steps of: (a) receiving at a

server the document as sent from a sender; (b) the server forwarding the document to a

recipient; (c) the document being forwarded to the recipient; and (d) the server receiving

instructions from the sender regards printing controls and the server implementing those

controls on the recipient (e.g. Fig. 1-3 col. 3, line 35-col. 5, line 35). Choudhury does

not explicitly disclose but Houser discloses document being authenticated to ensure its

integrity (e.g. col. 3, line 50-col. 4, line 19). It would have been obvious to one of

ordinary skill in the art at the time the invention was made to incorporate the document

verification process taught by Houser with Choudhury's secure document transmission

in order to verify the integrity, source and /or approval status of an electronic document

(Houser, col. 1, lines 5-20).

In respect to claim 2, Choudhury discloses a method for the remote printing a

document by use of a network, the method including the steps of: (a) a sender sending

the document to a server to enable the server to forward the document to a recipient;

(b) the document being authenticated by the sender prior to sending it to the server; and

(c) sending to the server instructions for controlling the printing of the document to

enable the server to implement those controls on the recipient (e.g. Fig. 1-3 col. 3, line

35-col. 5, line 35). Choudhury does not explicitly disclose but Houser discloses

document being authenticated to ensure its integrity (e.g. col. 3, line 50-col. 4, line 19).

It would have been obvious to one of ordinary skill in the art at the time the invention

was made to incorporate the document verification process taught by Houser with

Choudhury's secure document transmission in order to verify the integrity, source and

/or approval status of an electronic document (Houser, col. 1, lines 5-20).

In respect to claim 3, Choudhury discloses a method for printing of an

authenticated document received remotely by use of a network, the method including

the steps of: (a) a recipient receiving the authenticated document from a server, the

server having received the authenticated document from a sender; (b) the server

providing implementation of printing controls on the recipient, the server having received

the printing controls from the sender (e.g. Fig. 1-3 col. 3, line 35-col. 5, line 35).

Choudhury does not explicitly disclose but Houser discloses document being

authenticated to ensure its integrity (e.g. Houser, col. 3, line 50-col. 4, line 19). It would

have been obvious to one of ordinary skill in the art at the time the invention was made

to incorporate the document verification process taught by Houser with Choudhury's

secure document transmission in order to verify the integrity, source and /or approval

status of an electronic document (Houser, col. 1, lines 5-20).

In respect to claim 4, Choudhury and Houser disclose the method as claimed in

claim 1, wherein the printing controls include the ensuring that the document as printed

has a content that is exactly the same as the document content as sent by the sender

(e.g. Houser, col. 3, line 50-col. 4, line 19).

In respect to claim 5, Choudhury and Houser disclose the method as claimed in

claim 1, wherein the printing controls include anti-forgery controls (e.g. Choudhury, col.

3, line 65-col. 4, lines 43).

In respect to claim 6, Choudhury and Houser disclose the method as claimed in

claim 1, wherein the printing controls include anti-copying controls (e.g. Choudhury col.

3, lines 65-col. 4, line 43).

In respect to claim 7, Choudhury and Houser disclose the method as claimed in

claim 1. Choudhury and Houser do not explicitly disclose wherein the printing controls

include controls on a number of copies of the document that are to be printed.

However, control number of copies in printing control is old and well known. It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate controlling number of copy can be printed with the teaching of Choudhury's copyright control and Houser's teaching of document verification to prevent possible distribution of illicit copies.

In respect to claim 8, Choudhury and Houser disclose the method as claimed in claim 1, wherein the recipient includes a printer, the server providing the printing controls to the printer for the printing of the document, and the server enables a secure document delivery from the sender through the server to the recipient (e.g. Choudhury, col. 3, line 65-col. 4, line 42).

In respect to claim 9, Choudhury and Houser disclose the method as claimed in claim 8, wherein the server is a trusted agent to the sender in printing control, and is a trusted third party in document verification services (e.g. Choudhury, col. 3, lines 35-52).

In respect to claim 10, Choudhury and Houser disclose the method as claimed in claim 9, wherein the server stores a hash of the document, and at least one content feature of the document, and uses them for document verification (e.g. Houser, col. 2, lines 40-52).

In respect to claim 11, Choudhury and Houser disclose the method as claimed in claim 10, wherein secure document delivery and printing control is based on a trusted document structure including one or more from the group consisting of: a) the document itself; b) a hand signature; c) a digital signature; d) an optical watermark; e) content features of the document; f) usage control and audit trail; g) a seal of the sender; and h)

an expiry date (e.g. Houser, col. 4, lines 3-34).

In respect to claim 12, Choudhury and Houser disclose the method as claimed in claim 11, wherein the sender authorises the document (e.g. Houser, col. 4, lines 3-34).

In respect to claim 13, Choudhury and Houser disclose the method as claimed in claim 1, wherein the method uses a public key infrastructure to provide non-repudiation, privacy and security in the delivery of the document (e.g. Choudhury, col. 4, line 63-col. 5, line 10).

In respect to claim 14, Choudhury and Houser disclose the method as claimed in claim 11, wherein the digital signature is applied to the document, the digital signature being that of one or more selected from the group consisting of: the sender, the server, the recipient (e.g. Houser, col. 2, lines 40-61).

In respect to claim 15, Choudhury and Houser disclose the method as claimed in claim 1, wherein the sender is registered with the server before the sender can send the document, and the recipient is registered with the server before the recipient can receive the document (e.g. Choudhury, col. 3, lines 35-48 and col. 4, lines 1-12).

In respect to claim 16, Choudhury and Houser disclose the method as claimed in claim 11, wherein a document hash and the content features are sent with the document for validation, and a hash and content feature of the document are kept in the server for future verification (e.g. Houser, col. 12, lines 41-55).

In respect to claim 18, Choudhury and Houser disclose the method as claimed in claim 1, wherein the document as printed is protected against unauthorised copying and forgery by using an authentication means selected from the group consisting of: optical

watermark, special ink, special paper and special printing materials (e.g. Houser, col. 7,

lines 45-60). Choudhury and Houser do not explicitly disclose wherein the method uses

encryption techniques for secure document delivery, a key to decrypt the document

being sent directly to the recipient by a carrier means selected from the group consisting

of: email, telephone, mail, courier and personal delivery. However, communicating key

via email, telephone, mail courier or personal delivery is old and well known. It would

have been obvious to one of ordinary skill in the art at the time the invention was made

to incorporate this feature with the teaching of Choudhury's secure document

transmission and Houser's document verification so that secure key information would

not be transmitted via the same communication channel to prevent eavesdrop.

In respect to claim 19, Choudhury and Houser disclose the method as claimed in

claim 11, wherein the optical watermark has a counterfeit-proof layer, the printer being

calibrated to achieve a high level of performance of the counterfeit-proof layer (e.g.

Houser, col. 6, lines 25-41).

In respect to claim 20, Choudhury and Houser disclose the method as claimed in

claim 19, wherein the calibration is performed using a printing language without manual

intervention, the printer being secure in the printing control process (e.g. Houser, col. 6,

lines 25-41).

In respect to claim 21, Choudhury and Houser disclose the method as claimed in

claim 20, wherein the printer includes a secure memory, a secure central processing

unit, and a secure clock, the secure memory being used to store a private key, the

secure central processing unit being used to prevent run-time attacks; and the secure

clock being used to keep time (e.g. Choudhury, col. 5, line 37-col. 6, line 35).

In respect to claim 22, Choudhury and Houser disclose the method as claimed in claim 21, wherein the printer and the server system perform secure handshaking to authenticate each other, the printer and the server using one or more selected from the group consisting of a public key pair or the symmetry key of the printer (e.g. Choudhury, col. 5, line 37-col. 6, line 35).

In respect to claim 23, Choudhury and Houser disclose the method as claimed in claim 11, wherein the server sends an encrypted form of the document hash, the optical watermark, and printing instructions, to the printer (e.g. Houser, col.. 2, lines 30-60 and col. 7, lines 15-65).

In respect to claim 24, Choudhury and Houser disclose the method as claimed in claim 23, wherein the printer receives the document through client software, decrypts the document, and verifies the document with a hash and time stamp before printing, and adds the optical watermark during printing (e.g. Houser, col. 2, lines 30-60 and col. 7, lines 15-65).

In respect to claim 25, Choudhury and Houser disclose the method as claimed in claim 24. Choudhury and Houser do not explicitly disclose wherein the document is deleted from the secure memory immediately after printing, and an audit trail record is created in the server. However, deleting secure data in memory after accessing and storing of audit trail is old and well known. It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate this feature with teaching of Choudhury's secure document transmission and Houser's document

verification so that secure data would not be compromised for being stored in printer's memory after it has been read.

In respect to claim 26, Choudhury and Houser disclose the method as claimed in claim 1, wherein there is included client software that is downloaded to a machine of the recipient for the printing of the document, the recipient being trusted in the printing control process to minimise attack on the client software (e.g. Choudhury, col. 1, lines 35-60).

In respect to claim 27, Choudhury and Houser disclose the method as claimed in claim 26, wherein the server communicates with the printer through the client software to verify a serial number of a printer of a machine of the recipient and an internet protocol address of the recipient, check the status of the printer, locks a control panel of the printer, sets all necessary printer settings, sends to the printer the document and instructions for printing the document, and reset the printer settings after the printing process is completed, and creates an audit trail record in the server (e.g. Choudhury, col. 5, line 10-col. 6, line 67).

In respect to claim 28, Choudhury and Houser disclose the method as claimed in claim 11, wherein the seal includes one or more selected from the group consisting of: the hand signature and the seal; the seal including a common seal which is common to all printed copies, and a unique seal which is unique to each printed copy (e.g. Houser, col. 3, lines 15-45).

In respect to claim 29, Choudhury and Houser disclose the method as claimed in claim 26, wherein the client software has a basic part and a sensitive part, the sensitive

part being more susceptible to attack than the basic part; the basic part being sent to

the recipient when the recipient is registered with the server; the sensitive part being

downloaded to the recipient's machine for the printing of the document and is deleted

from the recipient's machine upon the completion of the printing to protect the sensitive

part from attack (e.g. Choudhury, col. 5, line 10-col. 7, line 48) .

In respect to claim 30, Choudhury and Houser disclose the method as claim in

claim 29, wherein an encrypted form of the sensitive part is sent to the recipient when

the recipient is registered with the server, the server managing the decryption key; the

sensitive part being decrypted when and as required (e.g. Choudhury, col. 5, line 10-col.

7, line 48).

In respect to claim 31, Choudhury and Houser disclose the method as claimed in

claim 29, wherein a hash result of the basic part is taken at the same time as or before

the basic part is sent to the recipient, the hash result being stored in the server; and

when the recipient requires printing of the document a second hash result of the basic

part is taken and compared with the hash result before printing is authorized by the

server (e.g. Houser, col. 2, lines 1-67).

In respect to claim 32, Choudhury and Houser disclose the method as claimed in

claim 27. Choudhury and Houser do not explicitly disclose wherein an execution time

for the execution of components of the sensitive part is recorded in the server, and

compared with the time taken for the execution of the components during the printing of

the documents; the printing being terminated if the time taken is significantly longer than

the execution time. Comparing timestamp to determine whether data has been

compromised is old and well known. It would have been obvious to one of ordinary skill

in the art at the time the invention was made to implement this feature with the teaching

of Choudhury's secure document transmission and Houser's document verification in

order to prevent secure data from malicious attack.

In respect to claim 33, Choudhury and Houser disclose the method as claimed in

claim 1, wherein the printing controls are implemented in response to the recipient

requesting the printing of the document (e.g. Choudhury, col. 5, lines 11-34).

In respect to claim 34, Choudhury and Houser disclose the method as claimed in

claim 1, Choudhury and Houser does not explicitly disclose wherein the printing control

is carried-out off-line, the server not participating in the printing process. However,

printing control carried out off line is old and well known. It would have been obvious to

one of ordinary skill in the art at the time the invention was made to implement this

feature with the teaching of Choudhury's secure document transmission and Houser's

document verification in event of network failure.

In respect to claim 35, Choudhury and Houser disclose the method as claimed in

claim 34, wherein there is provided a hardware device at the recipient to act on behalf of

the server (e.g. Choudhury, col. 5, line 12-col. 6, line 67, printing agent).

In respect to claim 36, Choudhury and Houser disclose the method as claimed in

claim 35, wherein the hardware device is for controlling the printing of the document, the

hardware device including a secure memory, a central processing unit with an on-chip

program, and an interface; the hardware device being registered with the server (e.g.

Choudhury, col. 5, line 12-col. 6, line 67, printing agent). Choudhury and Houser do not

explicitly discloses a delete after read memory. However, deleting secure data in memory after accessing is old and well known. It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate this feature with teaching of Choudhury's secure document transmission and Houser's document verification so that secure data would not be compromised for being stored in printer's memory after it has been read.

In respect to claim 37, Choudhury and Houser disclose the method as claimed in claim 35, wherein the recipient includes a printer, the hardware device being integral with the printer; the printer being registered with the server (e.g. Choudhury, col. 5, line 12-col. 6, line 67, printing agent).

In respect to claim 38, Choudhury and Houser disclose the method as claimed in claim 36, wherein the secure memory has an accessible memory that can be accessed only when a password of a user is entered and verified, the access being only to a block of the accessible memory relevant for that user; and a controlled memory for internal use, the controlled memory being divided into a plurality of blocks, there being one controlled memory block for each user (e.g. Choudhury, col. 6, lines 5-32).

In respect to claim 39, Choudhury and Houser disclose the method as claimed in claim 38, wherein the controlled memory is for the storage of secret keys, serial numbers, user's private keys and the recipient's ID key (e.g. Choudhury, col. 5, line 15-col. 6, line 67).

In respect to claim 40, the claim limitation is similar to claims 6 and 7. Therefore, claim 40 is rejected based on the similar rationale.

In respect to claim 41, Choudhury and Houser disclose the method as claimed in claim 40, wherein each license has a license key, the license key being used to encrypt the unique seal; the license keys being sent to the recipient by the server in an encrypted form and being installed in the hardware device (e.g. Choudhury, col. 5, line 15-col. 6, line 67).

In respect to claim 42, Choudhury and Houser disclose the method as claimed in claim 41, wherein the server can add to the number of license keys, the server generating a new license key set and a new top-up key, the new license key set and the new top-up key being encrypted with the previous top-up key prior to being sent to the recipient by the server and being installed in the hardware device (e.g. Choudhury, col. 5, line 15-col. 6, line 67).

In respect to claim 43, Choudhury and Houser disclose the method as claimed in claim 40, wherein each license includes an expiry date after which printing of the document using that license will no longer be possible (e.g. Choudhury, col. 5, line 15-col. 6, line 67).

In respect to claim 44, the claim limitation is similar to claim 18. Therefore, claim 44 is rejected based on the similar rationale.

In respect to claim 45, Choudhury and Houser disclose the method as claimed in claim 42, wherein the new license key set is sent with the document (e.g. Choudhury, col. 5, line 15-col. 7, 48).

In respect to claim 46, Choudhury and Houser disclose the method as claimed in claim 40, wherein prior to the sender sending the document, the sender's common seal,

a timestamp for sending, and the expiry date, are encrypted with a first session key to

give an encrypted result, and the encrypted result and the document are encrypted with

a second session key to give a second encrypted result (e.g. col. 5, line 15-col. 7, line

48).

In respect to claim 47, Choudhury and Houser disclose the method as claimed in

claim 46, wherein a hash result is included in the second encrypted result to provide a

means for checking data integrity (e.g. Houser, col. 2, line 29-67).

In respect to claim 48, Choudhury and Houser disclose the method as claimed in

claim 40, wherein the print controls can be to view the document but not to print the

document, a license not being required for viewing (e.g. Choudhury, col. 5, line 15-col.

7, line 48).

In respect to claim 49, the claim limitation is similar to claim 32. Therefore, claim

49 is rejected based on the similar rationale.

In respect to claim 50, Choudhury and Houser disclose the method as claimed in

claim 1, wherein the sender and the server are the same, all functions of the sender

being performed by the server (e.g. Choudhury, col. 3, line 35-col. 4, line 67).

4.   Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over

Choudhury et al. (U.S. Patent No. 5,509,074) in view of Houser et al. (U.S. Patent No.

5,606,609) and further in view of Reddy et al. (U.S. Patent No. 6,824,051).

In respect to claim 17, Choudhury and Houser disclose the method a claimed in

claim 1, wherein the authentication of the sender and the recipient is by using user

identity and at least one password (e.g. Choudhury, col. 5, lines 12-36). Choudhury

does not explicitly disclose but Reddy discloses uses a secure document transfer

channel provided by Secure Socket Layer protocol (e.g. Reddy, col. 5, lines 20-41). It

would have been obvious to one of ordinary skill in the art at the time the invention was

made to incorporate the teaching of secure document transmission taught by

Choudhury with the teaching of Secure Socket Layer Protocol taught by Reddy for a

secure communication channel.

5.   Claims 58-62 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Choudhury et al. (U.S. Patent No. 5,509,074).

In respect to claim 58, Choudhury and Houser disclose a hardware device for

use with a user's machine to enable control of printing of at least one document by the

machine, the hardware device including a secure memory, a central processing unit

with an on-chip program, and an interface. Choudhury does not explicitly disclose a

delete after read memory. However, deleting secure data in memory after accessing is

old and well known. It would have been obvious to one of ordinary skill in the art at the

time the invention was made to incorporate this feature with teaching of Choudhury's

secure document transmission so that secure data would not be compromised after it

has been read from the memory.

In respect to claim 59, Choudhury discloses the hardware device as claimed in

claim 58, wherein the secure memory has an accessible memory that can be accessed

only when a password of the user is entered and verified, the access being only to a

block of the accessible memory relevant for the user; and a controlled memory divided

into a plurality of blocks, there being one controlled memory block for each user (e.g.

Choudhury, col. 5, line 15-col. 7, line 48).

In respect to claim 60, Choudhury discloses the hardware device as claimed in

claim 59, wherein the controlled memory is for the storage of secret keys, serial

numbers, user's private keys, and the user's ID key (e.g. Choudhury, col. 5, lines 15-

67).

In respect to claim 61, Choudhury discloses the hardware device as claimed in

claim 58, wherein the hardware device is implemented as a secure software program

(e.g. Choudhury, col. 1, lines 35-60).

In respect to claim 62, Choudhury discloses the hardware device as claimed in

claim 61, wherein the software program is implemented in a distributed manner to assist

in preventing software attacks (e.g. Choudhury, col. 1, lines 35-61).

Allowable Subject Matter

6.   Claims 51-57 are objected to as being dependent upon a rejected base claim,

but would be allowable if rewritten in independent form including all of the limitations of

the base claim and any intervening claims.

Conclusion

7.   The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure.

-DeBry discloses a method and apparatus for transmitting status and control information from a printer to a print system.

-Palmer discloses a method and apparatus for generating a print stream from files optimized for viewing.

-DeBry discloses system, method and program for providing will-call certificates for guaranteeing authorization for a printer to retrieve a file directly from a file server upon request from a client in a network computer system environment.

-David et al. Disclose an apparatus and method for preventing disclosure through user authentication at a printing node.

-Gecht et al. Disclose a method and system for the provision of remote printing services over a network.

-DeBry discloses secure configuration of a digital certificate for a printer or other network device.

-Smith discloses method and apparatus for effecting secure document format conversion.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tongoc Tran whose telephone number is (571) 272-3843. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

Examiner: Tongoc Tran
Art Unit: 2134

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

TT

March 18, 2005